AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph beginning on page 4, line 10, of the submitted specification with the following amended paragraph:

[[6)]] 7) the CRT (Chinese Remainder Theorem) form of the private key is:

Please replace the paragraph beginning on page 8, line 17, of the submitted specification with the following amended paragraph:

According to a first variant, step A-1) consists [[in]] of calculating pairs of prime numbers (p,q) without knowledge of the public exponent e or of the length l of the key, using a parameter .PI. which is the product of small prime numbers. In this way, pair (p, q) obtained in step A has a maximum probability of being able to correspond to a future pair (e, l) and will make it possible to calculate a key d when step B is carried out.

Please replace the paragraph beginning on page 11, line 1, of the submitted specification with the following amended paragraph:

- a memory for storing the results of [[a]] step A consisting [[in]] of:

Please replace the paragraph beginning on page 11, line 10, of the submitted specification with the following amended paragraph:

- a program for implementing [[a]] step B consisting [[in]] of: